REMARKS/ARGUMENTS

Applicants respectfully request reconsideration and allowance of the pending claims. If the Examiner feels that a telephone conference would expedite the resolution of this case, he is respectfully requested to contact the undersigned.

Claim 12 was objected to due to a minor typo, the typo has been corrected, so it is believed that the noted objection has been overcome.

Claims 1-12 were rejected under 35 U.S.C. 101 as being directed to merely an abstract idea. Although the office action does not provide specific details to support the rejection, independent claim 1 has been amended to further clarify the claim language. It should be noted that as amended independent claim 1, claims a cryptographic system that includes at least one server. That should be more than enough to support the fact that claims 1-12 fall within statutory subject matter since they all claim "a machine" (a cryptographic system including at least one server, etc.) under 35 U.S.C. 101. As amended claims 1-12 are believed to overcome the noted rejection.

Claims 1-13 were rejected under 35 U.S.C. 103(a) as being unpatentable over Blakley et al, (U.S. Pat. No. 6,067,623) in view of the cited Microsoft Authenticode article (hereinafter referred to as the Article). The cited Blakley reference is directed to a system and method for controlling client access to enterprise resources using a middle tier server. According to Blakley, the middle tier server accesses resources "on behalf of a client by mapping the credentials used to access the server into credentials for accessing the resource" (see Col. 4, lines 18-22). The middle tier server (120) passes the user identity after the user has been authenticated to a credentials transfer (124) which maps the authenticated user's ID to an ID for the enterprise resource(s) the user needs to use using an ID map file (134, see Col. 5, lines 7-10). The Blakley reference provides the advantage that "the client has to authenticate once with the web server instead of requiring multiple logons with each enterprise resource" (see Col. 5, lines 22-24). The cited Article describes "Authenticode" a security feature that provides users the assurance of accountability and authenticity of signed

code before they download it from the internet (page 2, last paragraph). Authenticode uses digital signatures and certificates to assure the authenticity of signed code that is to be downloaded by a user.

Unlike the cited references, the present invention is directed to a cryptographic key administration scheme that uses cryptographic keys to manage confidential information on a database. The scheme uses one key (Integrity Key) configured within a Key Repository process to maintain the integrity of critical information on the database, and another key (Protection Key) is used to protect the confidential information on the database. The database works with the Key Repository process to enable any client application to work with any server process to service the request. Claim 1 has been amended to recite that the key repository process includes a database for storing the one or more than one set of symmetric keys, with each set of symmetric keys including an integrity key for ensuring the integrity of information stored in the database and a protection key configured to protect sensitive information on the database, the database storing there within operator entries used to retain the value of the integrity key and owner entries used to retain a share of the protection key.

Neither the Blakley reference nor the Article taken individually or in combination teach or suggest a cryptographic system using a key repository process as now claimed in the amended independent claim 1. The Blakely reference teaches a mapping technique using an ID mapping file (134), while the cited Article simply teaches assuring authenticity of files that are to be downloaded by using digital signatures and certificates. Neither reference teaches or suggests a key repository process including a database storing there within operator entries used to retain the value of the integrity key and owner entries used to retain a share of the protection key. The database works in conjunction with the key repository and provides a context storage mechanism that is very advantageous over the prior art methods of storing the context-related information in the working memory of the server or having the client store the context-related information in the form of cookies, etc. Given that neither of

the references teaches nor suggests a cryptographic system as now claimed in independent claim 1, it is believed that claims 1-12 are in condition for allowance.

Independent method claim 13 has been amended to further clarify the claim language and include that the key repository process includes a database for storing the one or more than one set of symmetric keys, each set of symmetric keys including an integrity key for ensuring the integrity of information stored in the database and a protection key configured to protect sensitive information on the database, the database storing there within operator entries used to retain the value of the integrity key and owner entries used to retain a share of the protection key.

Neither of the cited references taken individually or in combination teach or suggest a key repository process including a database for storing there within operator entries used to retain the value of an integrity key and owner entries used to retain a share of a protection key in a method for secure context-free multi-part communication in a computer system. As such, claim 13 is believed to be in condition for allowance.

New claims 14-18 have been introduced. It is believed given the above discussion relating to the cited references, that these new claims are also in condition for allowance.

In the course of the foregoing discussions, Applicants may have at times referred to claim limitations in shorthand fashion, or may have focused on a particular claim element. This discussion should not be interpreted to mean that the other limitations can be ignored or dismissed. The claims must be viewed as a whole, and each limitation of the claims must be considered when determining the patentability of the claims. Moreover, it should be understood that there may be other distinctions between the claims and the cited art which have yet to be raised, but which may be raised in the future.

Applicants respectfully request that a timely Notice of Allowance be issued in this case. If any fees or time extensions are inadvertently omitted or if any fees have been overpaid, please appropriately charge or credit those fees to Hewlett-

Appl. No. 09/736,715
Amdt. dated July 30, 2004
Reply to Office action of May 3, 2004

Packard Company Deposit Account Number 08-2025 and enter any time extension(s) necessary to prevent this case from being abandoned.

Respectfully submitted,

Pedro P. Hernandez
PTO Reg. No. 35,190
CONLEY ROSE, P.C.
(972) 731-2288 (Phone)
(972) 731-2289 (Fax)
ATTORNEY FOR APPLICANTS

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
Legal Dept., M/S 35
P.O. Box 272400
Fort Collins, CO 80527-2400